REMARKS

The Office Action dated February 20, 2008 has been received and carefully noted. The above amendments to the claims, and the following remarks, are submitted as a full and complete response thereto.

Claims 1-12, 14-24, and 26-31 have been amended to more particularly point out and distinctly claim the subject matter of the invention. Claim 25 has been cancelled without prejudice or disclaimer. New claims 32-52 have been added. No new matter has been added and no new issues are raised which require further consideration or search. Therefore, claims 1-12, 14-24, and 26-52 are currently pending in the application and are respectfully submitted for consideration.

The Office Action objected to claim 14, stating that claim 14 depends on a cancelled claim. (see Office Action at page 2, section 1). Claim 14 has been amended to depend upon claim 1, rather than claim 13. Applicants respectfully submit that said amendment to claim 14 moots the objection, and respectfully request that the objection be withdrawn.

The Office Action rejected claims 1-12, 14-21, and 25-26 under 35 U.S.C. § 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention. Specifically, the Office Action alleged that there is insufficient antecedent basis for the limitation "at least one message," in claims 1, 20-21, and 25-26. (see Office Action at page 2, section 2). Claim 25 has been cancelled. Claims 1, 20-21, and 26 have been amended to recite "the

communication comprising at least one message for the calling party," to provide the required antecedent basis. Applicants respectfully submit that said cancellation, and said amendments, moot the rejection, and respectfully request that the rejection be withdrawn.

The Office Action rejected claims 1-12, 14-16, 20-21, and 25-26 under 35 U.S.C. § 103(a) as allegedly being unpatentable over Tighe et al. (U.S. Patent No. 7,069,432) (hereinafter "Tighe"), in view of Applicant's alleged admitted prior art, paragraphs 0010-0015 of the specification (hereinafter "AAPA"). The Office Action took the position that Tighe discloses all the elements of the claims with the exception of "if the called party is not in the trusted network, the controlling comprises modifying at least one message for the called party," with respect to claim 1, "determining if the called party is in the trusted network comprises checking if the address is contained in the database provided in a call session control function or a security gateway," with respect to claim 6, "operating the first network and the second network in accordance with session initiation protocol," with respect to claim 16, and other limitations of the claims. The Office Action then cited AAPA as allegedly curing the deficiencies of Tighe.

Claim 25 has been cancelled, and Applicants respectfully submit that said cancellation moots the rejection, with respect to claim 25. Regarding the remaining claims, the rejection is respectfully traversed for at least the following reasons.

Claim 1, upon which claims 2-12 and 14-18 are dependent, recites a method, which includes determining, in a first network, an address associated with a called party of a second network. The method further includes determining based on the address if

the called party is in a trusted network. The method further includes controlling communication between the called party and a calling party of the first network based on if the called party is in the trusted network, the communication comprising at least one message for the called party, wherein if the called party is not in the trusted network, the controlling comprises modifying the at least one message.

Claim 20 recites a system, which includes a first determiner configured to determine an address associated with a called party located in a second network. The system further includes a second determiner configured to determine based on the address if the called party is in a trusted network. The system further includes a controller configured to control communication between the called party and a calling party, located in a first network, based on if the called party is in the trusted network, the communication comprising at least one message for the called party, wherein if the called party is not in the trusted network, the at least one message for the called party is modified.

Claim 21, upon which claims 32-49 are dependent, recites an apparatus, which includes a first determiner configured to determine an address associated with a called party located in another network. The apparatus further includes a second determiner configured to determine, based on the address, if the called party is in a trusted network. The apparatus further includes a controller configured to control communication between the called party and a calling party, located in a network where the apparatus is located, based on if the called party is in the trusted network, the communication comprising at

least one message for the called party, wherein if the called party is not in the trusted network, the at least one message for the called party is modified.

Claim 26 recites an apparatus, which includes first determining means for determining an address associated with a called party located in another network. The apparatus further includes second determining means for determining, based on the address, if the called party is in a trusted network. The apparatus further includes control means for controlling communication between the called party and a calling party based on if the called party, located in a network where the apparatus is located, is in the trusted network, the communication comprising at least one message for the called party, wherein if the called party is not in the trusted network, the at least one message for the called party is modified.

Claim 50 recites a computer program, embodied on a computer-readable medium, configured to control a processor to implement a method. The method includes determining, in a first network, an address associated with a called party of a second network. The method further includes determining based on the address if the called party is in a trusted network. The method further includes controlling communication between the called party and a calling party of the first network based on if the called party is in the trusted network, the communication comprising at least one message for the called party, wherein if the called party is not in the trusted network, the controlling comprises modifying the at least one message.

As will be discussed below, the combination of Tighe and AAPA fails to disclose or suggest all of the elements of the claims, and therefore fails to provide the features discussed above.

Tighe generally discloses a method for establishing a telephone call between a trusted Internet Protocol (IP) telephone and an untrusted device. The method includes receiving a call initiation request from the untrusted device that indicates a desired communication with the trusted IP telephone. The method evaluates the call initiation request, and establishes a telecommunication link between the untrusted device and the trusted IP telephone in response to a positive evaluation of the call initiation request. (see Tighe at Abstract).

AAPA, as discussed above, includes paragraphs 0010-0015 of the specification. AAPA generally discloses a Third Generation Partnership Project architecture for a third generation core network. (see Specification at paragraphs 0010-0015).

In a previous response, filed on November 15, 2007, (hereinafter "Previous Response") Applicants amended independent claim 1, to recite "wherein if the called party is not in the trusted network, the controlling comprises modifying at least one message for the called party." In the Previous Response, Applicants amended independent claims 20 and 21 similarly. Applicants further presented arguments in the Previous Response indicating that Tighe and AAPA fails to disclose said limitations of independent claims 1, 20-21 and 25-26. Specifically, Applicants argued that neither Tighe, nor AAPA, teaches or suggests that if the called party is not in a trusted network,

at least one message for the called party is modified. The currently pending Final Office Action maintained the rejection of independent claims 1, 20-21, and 25-26, without addressing Applicants' arguments. In fact, the currently pending Final Office Action failed to address any of Applicants' arguments. This is improper under the MPEP. As MPEP § 707.07(f) states, "[w]here the application traverses any rejection, the examiner should, if he or she repeats the rejection, take note of the applicant's argument and answer the substance of it. (MPEP § 707.07(f) – Answer All Material Traversed). As it stands, Applicants have no way of knowing whether the currently pending Final Office Action even took note of Applicants' arguments. Thus, Applicants respectfully request that a new non-final Office Action be issued, addressing Applicants' arguments in the Previous Response.

Notwithstanding the lack of response to Applicants' arguments, Applicants respectfully submit that Tighe and AAPA, whether considered individually, or in combination, fail to disclose, teach, or suggest, all of the elements of the present claims. For example, the combination of Tighe and AAPA fails to disclose, teach, or suggest, at least, "determining, in a first network, an address associated with a called party of a second network," "determining based on said address if said called party is in a trusted network," and "controlling communication between the called party and a calling party of the first network based on if said called party is in the trusted network, the communication comprising at least one message for the called party, wherein if the called party is not in the trusted network, the controlling comprises modifying the at least one

message," as recited in independent claim 1, and similarly recited in independent claims 20, 21, 26, and 50.

As discussed above, Tighe discloses a method for establishing a telephone call between a trusted Internet Protocol (IP) telephone and an untrusted device. Specifically, Tighe defines a "trusted device" as being an IP telephone that is coupled to a protected or trusted IP network being served by a telephone proxy such as telephone 24b in LAN 20, as depicted in Figure 1. (see Tighe at col. 9, lines 14-18; Figure 1). Tighe further defines a "untrusted device" as an IP or non-IP device that is external to a protected IP network. (see Tighe at col. 9, lines 18-20). Tighe further discloses that once a call initiation request has been received, the request is transferred to an authentication controller 25. The authentication controller determines if a trusted device is capable of receiving telephone calls. The authentication controller further determines whether the trusted device is a telephone by comparing a network address of the trusted device with addresses on a list, which contains IP addresses of telephones and other telephony devices that are permitted to receive calls from untrusted devices. (see Tighe at col. 9, lines 49-55; col. 10, lines 26-47).

The Office Action took the position that the authentication control in Tighe determining an address associated with a trusted device discloses, "determining, in a first network, an address associated with a called party of a second network," as recited in independent claim 1, and similarly recited in independent claims 20, 21, 26, and 50. (see Office Action at page 3, section 5). However, Tighe discloses that the determining takes

place in the same network as the network of the called party. Tighe fails to disclose or suggest that the determining takes place in a different network, as recited in the independent claims.

Additionally, Tighe fails to disclose, or suggest, "determining based on said address if said called party is in a trusted network," as recited in independent claim 1, and similarly recited in independent claims 20, 21, 26, and 50. As discussed above, Tighe merely discloses determining whether the called party is on a list containing addresses of telephones or other telephone devices. This list is provided in order to distinguish between telephones and other telephony devices, and other devices in the same trusted network, and does not distinguish whether the called party is in a trusted network.

Furthermore, Tighe fails to disclose "controlling communication between the called party and a calling party of the first network based on if said called party is in the trusted network," as recited in independent claim 1, and similarly recited in independent claims 20, 21, 26, and 50. Tighe discloses that any control of communication results from an evaluation of whether the called party is on a list of a subset of devices in a network, not based on whether the called party is in a particular network.

AAPA does not cure the deficiencies of Tighe. As discussed in the Previous Response, AAPA discloses that nodes in a trust domain are explicitly trusted by its users and end-systems to publicly assert the identify of each party. The nodes are also responsible for withholding that identity outside of the trust realm when privacy is recited.

Therefore, for at least the reasons discussed above, the combination of Tighe and AAPA fails to disclose, teach, or suggest, all of the elements of independent claims 1, 20, 21, 26, and 50. For the reasons stated above, Applicants respectfully request that this rejection be withdrawn.

Applicants further submit that the Office Action has failed to establish a prima facie case that independent claims 1, 20, 21, 26, and 50 are obvious in light of the cited references of Tighe and AAPA, because the Office Action has failed to establish a reasonable expectation of success.

As reiterated by the Supreme Court in *KSR International Co. v. Teleflex Inc.*, 550 U.S. ___, 82 USPQ2d 1385 (2007), the framework for the objective analysis for determining obviousness under 35 U.S.C. § 103 is stated in *Graham v. John Deere Co.*, 383 U.S. 1, 148 USPQ 459 (1966). Obviousness is a question of law based on underlying factual inquiries. The factual inquiries are: (a) determining the scope and content of the prior art; (b) ascertaining the differences between the claimed invention and the prior art; and (c) resolving the level of ordinary skill in the pertinent art. (see *KSR International Co. v. Teleflex Inc.*, 550 U.S. ___, 82 USPQ2d 1385 (2007); *Graham v. John Deere Co.*, 383 U.S. 1, 148 USPQ 459 (1966); see also MPEP § 2141).

The Supreme Court in *KSR* noted that the analysis supporting a rejection under 35 U.S.C. § 103 should be made explicit. The court stated that "rejections on obviousness cannot be sustained by mere conclusory statements; instead there must be some

articulated reasoning with some rational underpinning to support the legal conclusion of obviousness." (see *KSR*, 550 U.S. at ___, 82 UPSQ2d at 1396; see also MPEP § 2141).

As the Federal Circuit has stated, the rational to support a conclusion that a claim would have been obvious is that " a person of ordinary skill in the art would have been motivated to combine the prior art to achieve the claimed invention and that there would have been a reasonable expectation of success." (*DyStar Textilfarben GmbH & Co. Deutschland KG v. C.H. Patrick Co.*, 464 F.3d 1356, 1360, 80 USPQ2d 1641, 1645 (Fed. Cir. 2006)).

While the Office Action alleges a motivation to combine the references of Tighe and AAPA, the Office Action completely fails to allege a reasonable expectation of success in combining said references. Furthermore, Applicants respectfully submit that the cited references of Tighe and AAPA are directed toward different principles. Specifically, the operations disclosed in AAPA occur in the application layer, whereas the operations disclosed in Tighe occur at a lower layer. Additionally, Tighe relates to a way of allowing packets from untrusted sources to be delivered to telephones and telephony devices in a trusted network since typically such packets would not be able to infect the network or device with a virus, or other unwanted data, by receipt at a telephone or telephony device. In contrast, AAPA relates to messages from a trusted network coming into an untrusted network. Therefore, in light of the fundamental differences of Tighe and AAPA, Applicants respectfully submit that the combination of Tighe and AAPA would not result in a reasonable expectation of success.

Therefore, the Office Action has failed to establish a prima facie case that independent claims 1, 20, 21, 26, and 50 are obvious in light of the cited references of Tighe and AAPA.

Claims 2-12 and 14-16 depend upon independent claim 1. Claims 32-49 depend upon independent claim 21. Thus, Applicants respectfully submit that claims 2-12, 14-16, and 32-49 should be allowed for at least their dependence upon independent claims 1 and 21, respectively, and for the specific elements recited therein.

The Office Action rejected claims 17-19, 22-24, and 27-31 under 35 U.S.C. § 103(a) as being allegedly unpatentable over Tighe, in view of AAPA, and further in view of Peles (U.S. Publication No. 2004/0111642) (hereinafter "Peles"). The Office Action took the position that the combination of Tighe and AAPA discloses all the elements of the claims with the exception of "determining, in a first network, if there is a secure connection with a second network," and "modifying a message from a calling party to a called party if a determination is made that there is no secure connection with the second network," with respect to claim 22, and similar limitations with respect to claims 17 and 27. The Office Action then cited Peles as allegedly curing the deficiencies of Tighe and AAPA. The rejection is respectfully traversed for at least the following reasons.

Claim 22, upon which claims 23-24 are dependent, recites a method, which includes determining, in a first network, if there is a secure connection with a second network. The method further includes modifying a message from a calling party of the

first network to a called party of the second network if a determination is made that there is no secure connection with the second network.

Claim 27 recites an apparatus, which includes a determiner configured to determine if there is a secure connection with another network. The apparatus further includes a modifier configured to modify a message from a calling party of a network where the apparatus is located to a called party of the other network if a determination is made that there is no secure connection with the another network.

Claim 28 recites an apparatus, which includes determining means for determining if there is a secure connection with another network, and modifying means for modifying a message from a calling party of a network where the apparatus is located to a called party of the another network if a determination is made that there is no secure connection with the another network.

Claim 29 recites a method, which includes determining, in a gateway in a first network, if there is a secure connection with a second network. The method further includes discarding a message from a calling party in a first network to a called party in a second network, if a determination is made that there is no secure connection with the second network.

Claim 30 recites an apparatus, which includes a determiner configured to determine, in a gateway, if there is a secure connection with another network. The apparatus further includes a discarder configured to discard a message from a calling

party of a network where the apparatus is located to a called party of the another network if a determination is made that there is no secure connection with the another network.

Claim 31 recites an apparatus, which includes determining means for determining, in a gateway, if there is a secure connection with another network . The apparatus further includes discarding means for discarding a message from a calling party of a network where the apparatus is located to a called party of the another network if a determination is made that there is no secure connection with the another network.

Claim 51 recites a computer program, embodied on a computer-readable medium, configured to control a processor to implement a method. The method includes determining, in a first network, if there is a secure connection with a second network. The method further includes modifying a message from a calling party of the first network to a called party of the second network if a determination is made that there is no secure connection with the second network.

Claim 52 recites a computer program, embodied on a computer-readable medium, configured to control a processor to implement a method. The method includes determining, in a gateway in a first network, if there is a secure connection with a second network. The method further includes discarding a message from a calling party in a first network to a called party in a second network, if a determination is made that there is no secure connection with the second network.

As will be discussed below, the combination of Tighe, AAPA, and Peles fails to disclose or suggest all of the elements of the claims, and therefore fails to provide the features discussed above.

The descriptions of Tighe and AAPA, as discussed above, are incorporated herein. Peles generally discloses a security switch that detects whether requested content is either trusted content or non-trusted content. When the network content is trusted content, network traffic bypasses the inspection gateway and goes directly to the user. When the network content is non-trusted content, network traffic passes through to the inspection gateways for inspection. (see Peles at Abstract).

Applicants respectfully submit that Tighe, AAPA, and Peles, whether considered individually or in combination, fail to disclose, teach, or suggest, all of the elements of the present claims. For example, the combination of Tighe, AAPA, and Peles fails to disclose, teach, or suggest, at least, "determining, in a first network, if there is a secure connection with a second network," and "modifying a message from a calling party of the first network to a called party of the second network if a determination is made that there is no secure connection with said second network," as recited in independent claim 22, and similarly recited in independent claims 27, 28, and 51; and "determining, in a gateway in a first network, if there is a secure connection with a second network," and "discarding a message from a calling party in a first network to a called party in a second network, if a determination is made that there is no secure connection with said second

network," as recited in independent claim 29, and similarly recited in independent claims 30, 31, and 52.

The Office Action correctly concludes that Tighe and AAPA fails to disclose, or suggest, the limitations recited above.

Regarding claims 22, 27, 28, and 51, Peles does not cure the deficiencies of Tighe and AAPA. As discussed in the Previous Response, Peles fails to disclose a "secure connection," as recited in independent claims 22, 27, 28, and 51. Instead, Peles merely discloses a security switch which parses an incoming request, identifies a file name extension, and verifies if the file name extension is a trusted extension by comparing it against a maintained list of trusted extensions. (see Peles at paragraph 0047). Applicants respectfully submit that the cited paragraph of Peles fails to disclose a "secure connection," because one of ordinary skill in the art would readily understand that a "secure connection" is a connection that is resistant to interception or tampering. The cited paragraph of Peles fails to disclose such a connection.

Furthermore, Peles fails to disclose, or suggest, "modifying a message," as recited in independent claim 22, and similarly recited in independent claims 27, 28, and 51. Instead, Peles merely discloses that if the security switch determines that the file extension falls under the "non-trusted" file extension category, the security switch sends the file extension to the inspection gateway rather directly to the server. (see Peles at paragraph 0047). Thus, Peles merely teaches diverting a message, not modifying the message.

Regarding claims 29-31 and 52, Peles also does not cure the deficiencies of Tighe and AAPA. The Office Action takes the position that, "regarding claims 29-31, these claims have similar limitations as claim 22." (see Office Action at page 9). However, Applicants respectfully submit that claims 29-31 and 52 clearly have limitations that are not found in claim 22. For example, claim 29 recites "discarding a message from a calling party in a first network to a called party in a second network," which does not appear in claim 22. Furthermore, claim 29 recites "determining, in a gateway in a first network, if there is a secure connection with a second network," whereas claim 22 recites "determining, in a first network, if there is a secure connection with a second network." Claims 30-31 and 52 have similar differences from claim 22. Thus, the Office Action has failed to establish that the combination of Tighe, AAPA, and Peles discloses all of the elements of independent claims 29-31 and 52.

Therefore, for at least the reasons discussed above, the combination of Tighe, AAPA, and Peles fails to disclose, teach, or suggest, all of the elements of independent claims 22, 27-31, and 51-52. For the reasons stated above, Applicants respectfully request that this rejection be withdrawn.

Claims 23-24 depend upon independent claim 22. Thus, Applicants respectfully submit that claims 23-24 should be allowed for at least their dependence upon independent claim 22, and for the specific elements recited therein.

Applicants further submit that the Office Action has failed to establish a prima facie case that independent claims 22, 27-31, and 51-52 are obvious in light of the cited

references of Tighe, AAPA, and Peles, because the Office Action has failed to establish a reasonable expectation of success.

While the Office Action alleges a motivation to combine the references of Tighe AAPA, and Peles, the Office Action completely fails to allege a reasonable expectation of success in combining said references. Furthermore, Applicants respectfully submit that the cited references of Tighe, AAPA, and Peles are directed toward different principles. Specifically, Peles relates to a prevention of an attack on a client by monitoring the extensions of incoming content, and if an extension is not trusted, diverting the content bearing that extension. In contrast, Tighe relates to call set up, and AAPA releates to privacy at the edge of trust domains. More specifically, Peles relates to examination of an HTML file name extension, whereas Tighe relates to examination of a network address, and AAPA relates to examination of a SIP header.

Moreover, any attempt to combine the teachings would lead to failure, as the disclosures are incompatible. Specifically, a SIP entity, as in AAPA, cannot "discard" content bearing an HTML file name extension, as taught in Peles. Therefore, in light of the fundamental differences of Tighe, AAPA and Peles, Applicants respectfully submit that the combination of Tighe, AAPA, and Peles would not result in a reasonable expectation of success.

Therefore, the Office Action has failed to establish a prima facie case that independent claims 22, 27-31, and 51-52 are obvious in light of the cited references of Tighe, AAPA, and Peles.

Regarding claims 17-19, said claims depend upon independent claim 1. As discussed above, the combination of Tighe and AAPA does not disclose, teach, or suggest all of the elements of independent claim 1 Furthermore, Peles does not cure the deficiencies in Tighe and AAPA, as Peles also does not disclose, teach, or suggest, at least, "determining, in a first network, an address associated with a called party of a second network," "determining based on said address if said called party is in a trusted network," and "controlling communication between the called party and a calling party of the first network based on if said called party is in the trusted network, the communication comprising at least one message for the called party, wherein if the called party is not in the trusted network, the controlling comprises modifying the at least one message," as recited in independent claim 1. Thus, the combination of Tighe, AAPA, and Peles does not disclose, teach, or suggest all of the elements of claims 17-19. Additionally, claims 17-19 should be allowed for at least their dependence upon independent claim 1, and for the specific elements recited therein.

For at least the reasons discussed above, Applicants respectfully submit that the cited prior art references fails to disclose or suggest all of the elements of the claimed invention. These distinctions are more than sufficient to render the claimed invention unanticipated and unobvious. It is therefore respectfully requested that all of claims 1-12, 14-24, and 26-52 be allowed, and this application passed to issue.

If for any reason the Examiner determines that the application is not now in condition for allowance, it is respectfully requested that the Examiner contact, by

telephone, the applicants' undersigned attorney at the indicated telephone number to arrange for an interview to expedite the disposition of this application.

In the event this paper is not being timely filed, the applicants respectfully petition for an appropriate extension of time. Any fees for such an extension together with any additional fees may be charged to Counsel's Deposit Account 50-2222.

Respectfully submitted,

Majid S. AlBassam
Registration No. 54,749

Customer No. 32294
SQUIRE, SANDERS & DEMPSEY LLP
14TH Floor
8000 Towers Crescent Drive
Tysons Corner, Virginia 22182-2700
Telephone: 703-720-7800
Fax: 703-720-7802

KMM:dc:dlh

Enclosures: Additional Claim Fee Transmittal
Check No. 018842